WHAT IS CLAIMED IS:

1. A method comprising:

in a server, hosting an intrusion detection process that provides intrusion detection services; and

integrating the intrusion detection process with a server process.

2. The method of claim 1 in which integrating comprises:

defining global application programmer interface (API) structures in the intrusion detection process to establish a connection to an application programmer interface (API) of the server process.

3. The method of claim 2 further comprising:

passing a request for data received by the server to the intrusion detection process.

4. The method of claim 3 in which the intrusion detection process comprises:

packing a subset of the data into an analysis format; and

passing the subset to an analysis process.

5. The method of claim 4 further comprising analyzing the subset in the analysis process.

6. The method of claim 1 in which the server is a web server.

7. The method of claim 6 in which the web server is an Apache web server.

8. The method of claim 4 in which the analysis process is resident in the web server.

9. The method of claim 4 in which the analysis process is resident outside of the web server.

10. The method of claim 4 in which passing further comprises delivering the subset in a funneling process via a socket.

11. The method of claim 10 in which the funneling process comprises:

accepting incoming connections to which the subset can be transmitting; and

passing the subset to outgoing connections.

12. A method comprising:

passing a request for data received by a first server process executing in a first server to a detection process that includes:

packing a subset of the data into an analysis format; and

passing the subset to an analysis process.

13. The method of claim 12 also including

analyzing the subset in the analysis process.

14. The method of claim 12 in which passing comprises passing control from the first server through an Application Programming Interface (API) of a server program.

15. The method of claim 12 in which the first server comprises a web server.

16. The method of claim 12 in which the detection process is resident in the first server.

17. The method of claim 13 in which the analysis process is resident in the first server.

18. The method of claim 13 in which the analysis process is resident in a second server.

19. The method of claim 12 in which the analysis format comprises an Emerald format.

20. The method of claim 12 in which the analysis process comprises an Emerald eXpert analysis process.

21. The method of claim 15 in which the web server comprises an Apache web server.

22. The method of claim 21 in which the passing further comprises:

receiving the subset in a piped logs interface of the Apache web server; and

delivering the subset to a funneling process via a socket.

23. The method of claim 22 in which the funneling process comprises:

accepting incoming connections to which the subset can be transmitted; and

passing the subset to outgoing connections.

24. The method of claim 22 in which the funneling process further comprises duplicating the subset for delivery to a second analysis process.

25. A system comprising:

a web server process having an application programming interface (API); and

an intrusion detection process linked to the API.

26. The system of claim 25 further comprising a link to an external system having an analysis process.

27. The system of claim 26 in which the intrusion detection process comprises:

receiving a request for data;

packing a subset of the data into a common analysis format;

passing the subset to the analysis process; and

analyzing the subset in the analysis process.

28. The system of claim 25 in which the web server process is an Apache web server process.

29. The system of claim 26 in which the common analysis format is an Emerald format.

30. The system of claim 26 in which the analysis process is an Emerald analysis process.

31. A computer program product residing on a computer readable medium having instructions stored thereon which, when executed by the processor, cause the processor to:

receive a request for data;

pack a subset of the data into a common analysis format;

pass the subset to an analysis process; and

analyze the subset in an analysis process.

32. A processor and a memory configured to:

receive a request for data;

pack a subset of the data into a common analysis format;

pass the subset to an analysis process; and

analyze the subset in an analysis process.

33. A computer program product residing on a computer readable medium having instructions stored thereon which, when executed by the processor, cause the processor to:

integrate an intrusion detection process with a server process.

34. A processor and memory configured to:

integrate an intrusion detection process with a server process.